



UNITED STATES MARINE CORPS  
MARINE CORPS SYSTEMS COMMAND  
2200 LESTER STREET  
QUANTICO VIRGINIA 22134-5010

IN REPLY REFER TO

5720  
DON-USMC-2022-009932  
5 Jul 22

**Sent via email to: [foia@foia.com](mailto:foia@foia.com)**

FOIA Group  
Ms. Rose Santos  
PO Box 368  
Depew NY 14043

SUBJECT: FOIA DON-USMC-2022-009932

Dear Ms. Santos:

This responds to your FOIA request dated June 28, 2022, which requests a copy of "Relevant to 47QTCK18D0037 Order M6785422F4011, we seek CLEARLY RELEASABLE copies of the following: (1) Task order title page (1st page only) and (2) the Task Order's CURRENT Statement of Work/Performance Work Statement (SOW/PWS)."


The requested documents are enclosed.

Fees associated with processing your request are minimal and waived.

Any questions concerning this matter should be directed to Mrs. Bobbie Cave at (703) 432-3934 or [bobbie.cave@usmc.mil](mailto:bobbie.cave@usmc.mil).

Sincerely,

*Bobbie Cave*  
for Lisa L. Baker  
Counsel

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS</b> <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30</i>				1. REQUISITION NUMBER SEE SCHEDULE		PAGE 1 OF 84	
2. CONTRACT NO. 47QTC18D0037		3. AWARD/EFFECTIVE DATE 25-Mar-2022		4. ORDER NUMBER M6785422F4011		5. SOLICITATION NUMBER M6785421R4011	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME DOMINIQUE N. BARR				b. TELEPHONE NUMBER (No Collect Calls) 703-432-7409	
9. ISSUED BY COMMANDER, MARINE CORPS SYSTEMS COMMAND ATTN: DOMINIQUE BARR 2200 LESTER STREET QUANTICO VA 22134  TEL: 703-432-7409 FAX:		CODE M67854		10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> SERVICE-DISABLED <input type="checkbox"/> EDWOSB <input type="checkbox"/> VETERAN-OWNED <input type="checkbox"/> 8(A) NAICS: 541519 SIZE STANDARD: \$30,000,000			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS Net 30 Days		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING	
				14. METHOD OF SOLICITATION <input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input checked="" type="checkbox"/> RFP			
15. DELIVER TO COMMANDER MARCORSYSCOM REGINA WASHINGTON 2200 LESTER ST. QUANTICO VA 22134		CODE M67854		16. ADMINISTERED BY  <b>SEE ITEM 9</b>			
17a. CONTRACTOR/ OFFEROR TYTO GOVERNMENT SOLUTIONS, INC. LISA SINGLETARY 510 SPRING ST STE 200 HERNDON VA 20170-5148 TELEPHONE NO. 703-935-6010		CODE 7N699 FACILITY CODE		18a. PAYMENT WILL BE MADE BY DFAS COLUMBUS HQ0871 P.O.BOX 360922 COLUMBUS OH 43213-9022			
<input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM					
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	<b>SEE SCHEDULE</b>						
25. ACCOUNTING AND APPROPRIATION DATA  <b>See Schedule</b>					26. TOTAL AWARD AMOUNT (For Govt. Use Only)  <b>\$4,727,877.20</b>		
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED							
<input checked="" type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input checked="" type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED							
<input checked="" type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.  REF: Proposal 18175				<input type="checkbox"/> 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: SEE SCHEDULE			
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)  			
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) STASIA BAKER / CONTRACTING OFFICER TEL: 703-432-8327 EMAIL: stasia.baker@usmc.mil		31c. DATE SIGNED 24-Mar-2022	

## PERFORMANCE WORK STATEMENT

### **Performance Work Statement (PWS) Information Technology Service Management (ITSM) Tools Operations and Sustainment (O&S)**

#### 1.0 Introduction

The purpose of this document is to provide a Performance Work Statement (PWS) for the Marine Corps Information Technology Service Management (ITSM) Tools Operations and Sustainment (O&S).

#### 1.1 Background

The Marine Corps is dedicated to continuous successful implementation of ITSM Services using best practices and supporting tools. In support of this vision, the Marine Corps is working to establish a comprehensive, integrated ITSM implementation based on the Department of Defense (DoD) Enterprise Service Management Framework (DESMF) as specified in Department of Defense Instruction (DoDI) 8440.01. This requires implementing industry best practices while conforming to Department of Defense (DoD), Department of Navy (DON), and United States Marine Corps (USMC) standards, policies, and guidance.

The Marine Corps' vision, strategy, and planning documents, intended to unify and synchronize the efforts of the Marine Corps Information Technology (IT) community, are the Enterprise ITSM (E-ITSM) Campaign Plan, Marine Corps Information Environment Enterprise (MCIEE) Blueprint, and Commandant's Planning Guidance.

The ITSM Tool Suite is in place to support the Information Technology Infrastructure Library (ITIL) based processes for the Marine Corps classified and unclassified garrison information environments. These tools provide the vehicle to assist in the automation and management of E-ITSM processes, architectures, roles, and responsibilities. The Marine Corps E-ITSM implementation includes the activities outlined in the following domains and processes:

1. Service Strategy Domain
  - a. Strategy Generation Management Process
  - b. Business Relationship Management Process
  - c. Service Portfolio Management Process
  - d. Financial Management Process
  - e. Demand Management Process
  - f. Service Catalog Management Process
2. Service Design Domain
  - a. Design Coordination Process

- b. Supplier Management Process
  - c. Information Security Management Process
  - d. IT Service Continuity Management Process
  - e. Availability Management Process
  - f. Capacity Management Process
  - g. Service Level Management Process
- 3. Service Transition Domain
  - a. Transition Planning & Support Process
  - b. Release and Deployment Management Process
  - c. Change Evaluation Process
  - d. Service Validation and Testing Process
  - e. Asset Management Process
  - f. Configuration Management Process
  - g. Change Management Process
  - h. Knowledge Management Process
- 4. Service Operation Domain
  - a. Problem Management Process
  - b. Access Management Process
  - c. Event Management Process
  - d. Incident Management Process
  - e. Request Fulfillment Process

#### 1.1.1 ITSM Tool Suite

The ITSM tool suite that supports USMC E-ITSM processes is built on BMC applications with an Oracle database backend running on Red Hat Enterprise Linux (RHEL) and Microsoft Windows servers.

BMC Remedy is the service management platform used for tracking and managing USMC IT processes, activities, and assets. BMC Remedy enables multiple process areas to manage data specific to their process while allowing each process to seamlessly share and relate information and activities through record association. The capability of the Remedy tool provides for the creation and storage of various types of records, including incident records, problem records, change records, release records, request records, asset records, contract and warranty records, and software license records. BMC Remedy provides reporting and dash-boarding capabilities for all system records, attributes and data elements. BMC Remedy also houses a searchable repository of knowledge articles that can be associated with designated system modules, workflows, and custom applications.

The Marine Corps established an enterprise Configuration Management Database (CMDB) using BMC Atrium controlled within the enterprise Service Asset and Configuration Management (SACM) process. The USMC CMDB stores all USMC asset and Configuration Items (CI) records. The goal is to provide a clear picture of enterprise physical and virtual assets including their relationship to each other. The Marine Corps implemented a custom BMC Remedy Tech Refresh workflow automation within the Asset Management console that allowed regional Asset Managers the “enhanced” ability to plan and execute major non-data center asset refreshes across the enterprise.

In addition to the Tech Refresh workflow, the Marine Corps is working to establish IT license management capabilities for software licenses procured by the Strategic Sourcing Services portfolio in the Portfolio Management (PfM), Marine Corps Supporting Establishment Systems (MCSES), Program Executive Office for Digital and Enterprise Services (PEO Digital). This includes tracking of software license compliance in Remedy using the contracts module, asset inventory data, and network-discovered data of desktops and laptops stored in the CMDB.

As part of providing IT Services<sup>1</sup> for the USMC, the Marine Corps has established an enterprise service catalog comprising of orderable technical enterprise services. USMC has integrated the Service Request Module with Work Order Management allowing users requesting services to have a fully transparent view from ordering through fulfillment.

---

<sup>1</sup> ITSM terms like Service and Process are defined in the DESMF as prescribed by DoDI 8440.01.

The Marine Corps has also developed and delivered Computer-Based Training (CBTs), Job Aids, and Just-in-Time (JIT) videos in order to explain ITSM processes and their supporting toolsets. These CBTs and JIT videos ensure that the operator and the Warfighter have adequate ITSM training.

#### 1.1.2 Current State of ITSM Tools

Under the federal cybersecurity Risk Management Framework (RMF), the ITSM tools are categorized for Confidentiality, Integrity, and Availability as Medium-Medium-Low.

The ITSM toolset suite is installed, configured, and customized according to Marine Corps ITSM Technical Data Packages (TDPs) and the Marine Corps' Hybrid Cloud Services (HCS) technical documentation and will be provided as GFI. HCS is the program of record for providing Marine Corps hosting services in the Kansas City Data Center.

USMC personnel are ITSM trained in accordance with existing Marine Corps ITSM Training Documentation including CBT, Job Aids, Just-in-Time videos, and other training documents.

The Marine Corps ITSM Service Catalog is housed in the BMC Remedy Service Request Management (SRM) module and is populated with an orderable set of services related to enterprise hardware and software.

Many Request Fulfillment (RqF) workflows, including Hardware and Software ordering, are implemented within the Remedy Service Request Module, a custom application that receives and manages all orders placed via the USMC Product Ordering service request. The RqF capability also enables integration with the Information Technology Procurement Request Review/Approval System (ITPRAS) (service request approval system), which is built as a module in Remedy.

The Knowledge Management module in Remedy contains over 5,000 Knowledge articles with the ability to create, review, and approve new articles and search existing articles. It is integrated with the Remedy Service Request, Incident, and Problem Management modules.

Mail Integration enables the system to send outgoing email to users receiving Remedy record assignment. Incoming email replies are received by Remedy and recorded into the work detail fields of the corresponding record.

##### 1.1.2.1 Existing ITSM Toolset Environments

Several ITSM Toolset environments have been set up to support engineering and testing of enhancements within the solution and training on changes to the tool prior to fielding into production on the operational Marine Corps Enterprise Network (MCEN).

- uPROD – Unclassified Production environment that employees and authorized personnel use for day to day work. It is also referred to as unclassified EITC (uEITC) and is connected to the MCEN Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNet) and also available externally via CAC. This environment consists of 20 servers and 7 databases with the following general descriptions:
  - 6 Application servers (MS Windows 2012 R2)
  - 5 Mid-tier servers (MS Windows 2012 R2)
  - 2 Smart Reporting servers (MS Windows 2012 R2)
  - 2 Digital Work Place Application servers (MS Windows 2012 R2)
  - 2 Digital Work Place Catalog servers (RHEL 7.8)
  - 2 Smart IT servers (Windows 2012 R2)
  - 1 Definitive Media Library file server (RHEL 7.8)
  - 7 Oracle Database Instances (hosted by HCS) (Oracle 12c on RHEL 7.8)
- cPROD – Classified Production environment on the secure network. This is also known as the Classified EITC (cEITC). This requires MCEN Secret IP Router Network (SIPRnet) access permissions. This environment consists of 15 servers and 7 databases with the following general descriptions:
  - 4 Application servers (MS Windows 2012 R2)
  - 3 Mid-tier servers (MS Windows 2012 R2)
  - 2 Smart Reporting servers (MS Windows 2012 R2)

- 2 Digital Work Place Application servers (MS Windows 2012 R2)
  - 2 Digital Work Place Catalog servers (RHEL 7.8)
  - 2 Smart IT servers (Windows 2012 R2)
  - 7 Oracle Database Instances (hosted by HCS) (Oracle 12c on RHEL 7.8)
- ZONE A - HCS hosted pre-production environment. This is the official test and integration environment for systems that are transitioning into the HCS production environments. This environment consists of 12 servers and 7 databases with the following general descriptions:
  - 3 Application servers (MS Windows 2012 R2)
  - 3 Mid-tier servers (MS Windows 2012 R2)
  - 2 Smart Reporting servers (MS Windows 2012 R2)
  - 1 Digital Work Place Application server (MS Windows 2012 R2)
  - 1 Digital Work Place Catalog server (RHEL 7.8)
  - 1 Smart IT server (Windows 2012 R2)
  - 1 Definitive Media Library file server (RHEL 7.8)
  - 7 Oracle Database Instances (hosted by HCS) (Oracle 12c on RHEL 7.8)
- HCS Remedy Training Stack - Online copy of the production Remedy suite with test data used for validation and training hosted at HCS Zone A and available on the Marine Corps Enterprise Network – Non-classified Internet Protocol (IP) Router Network (MCEN-N). This environment consists of 7 servers and 7 databases with the following general descriptions:
  - 1 Application server (MS Windows 2012 R2)
  - 1 Mid-tier server (MS Windows 2012 R2)
  - 1 Smart Reporting servers (MS Windows 2012 R2)
  - 1 Digital Work Place Application servers (MS Windows 2012 R2)
  - 1 Digital Work Place Catalog servers (Red Hat Enterprise Linux 7.8)
  - 1 Smart IT servers (Windows 2012 R2)
  - 1 Definitive Media Library file server (Red Hat Enterprise Linux 7.8)
  - 7 Oracle Database Instances (hosted by HCS) (Oracle 12c on RHEL 7.8)
- Contractor Tools Configuration Sandbox Environment – A tools configuration enhancement stack hosted by the incumbent contractor at the contractor facility utilizing contractor property. This environment will be decommissioned as part of current contract closeout. The replacement tools configuration enhancement environment will be within the Marine Corps Systems Command (MCSC) Enterprise Engineering and Verification Environment (EEVE) lab as defined in Section 2.6.

#### 1.1.2.2 Existing ITSM Toolset Assessment and Authorization (A&A):

Production ITSM tools on the operational MCEN in the uEITC, cEITC, and Zone A are covered under an overarching Authority to Operate (ATO).

#### 1.1.2.3 Existing ITSM Toolset System Interfaces:

The USMC ITSM Toolset relies heavily on authoritative data from other systems. This data is integrated into the CMDB using technologies such as Atrium Integrator Pentaho plug-in and the Seamless Data Pump for BMC Atrium CMDB. The following sources are examples of current interfaces that provide CMDB data integration:

- System Center Configuration Manager (SCCM) polls USMC desktops and laptops for asset information, which populates the BMC Atrium CMDB.
- VMware vCenter provides virtualization infrastructure data for regional virtualization environments and includes limited server configuration data, which populates the BMC Atrium CMDB.
- Blackberry User Enterprise Management (BUEM) provides mobile device asset data, which populates the BMC Atrium CMDB.
- Microsoft Active Directory (AD) is the authoritative source of information for organizational structures and enterprise user accounts. AD user accounts populate ITSM system accounts.

### 1.3 Scope

The contractor shall provide ITSM Tools O&S for the United States Marine Corps (USMC) as defined in this PWS. Operations and Sustainment efforts include assisting the Government in expanding and sustaining Marine Corps ITSM Tool capabilities across the enterprise, and supporting Marine Corps ITSM Tool operations in all environments listed in Section 1 in accordance with requirements. The contractor's primary role is to support and

enhance the Government's ability to operate the ITSM tool in direct support of EITSM processes. This scope includes planning, developing and documenting system enhancements, supporting documentation updates, configuration management of the system, systems engineering and testing activities, operational support, integration, installation, Assessment and Authorization (A&A), training, and maintenance. The task also covers implementation and support services for the Government-owned software tools that support these processes.

## CDRL A00A Assessment and Authorization Documentation and Artifacts

### 1.3.1 Place of Performance

The primary place of performance for this contract will be in the National Capital Region and Government facilities on Marine Corps Base (MCB) Quantico, VA. Operational support shall be staffed at the Marine Corps Cyber Operations Group (MCCOG). Engineering and testing support shall be staffed at MCSC.

The Government will provide desk space and telephones within these facilities for all contractors supporting the objectives, as well as required badges and accesses that have been approved. Additional details regarding Government Furnished Equipment (GFE) are listed in Section 4.0.

Tasks involving live operational support and deployment shall be conducted at the MCCOG. Tasks involving engineering, design, system configuration/enhancement and testing shall be conducted at the MCSC Lab.

### 1.3.2 Post Award Conference/Periodic Progress Meetings

The contractor shall attend a post award conference (PAC) approximately 30 days after contract award. The purpose of the PAC is for the contractor to review and demonstrate to the Government the management procedures, review of technical and other specialty area support capabilities, and to establish schedule dates for near term critical meetings/actions. The contractor shall present an overview of their plans, key personnel, and program implementation processes. The PAC is also an opportunity to: (1) aid both the Government and contractor personnel in achieving a clear and mutual understanding of all requirements; and (2) identify and resolve potential problems. The Contracting Officer (KO), Contracting Officer Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance at least semi-annually.

## 2.0 Performance Requirements

### 2.1 Program Management

The Contractor shall plan and execute all work required under this PWS.

#### 2.1.1 Kick Off Meeting

The contractor shall attend a Government Kick Off Meeting within ten working days after TO award. The meeting will be held in the greater Quantico, VA area. It is anticipated that the Kick Off meeting will be no more than one work day in duration. It shall include, but not be limited to, an overview of requirements; quality assurance and acceptance procedures; personnel and physical security issues; data and deliverable structure or format; and other potential issues or problems.

#### 2.1.2 Integrated Master Schedule

The contractor shall deliver an IMS that encompasses the entire scope of the TO to include Government dependencies.

CDRL A001 Integrated Master Schedule

#### 2.1.3 Work Breakdown Structure (WBS), Program Management Plan and Staffing Plan

The contractor shall deliver a WBS, Program Management Plan and Staffing Plan.

CDRL A002 Work Breakdown Structure

CDRL A003 Program Management Plan

CDRL A005 Staffing Plan

#### 2.1.4 Risk Management Plan

The contractor shall provide a Risk Management Plan (RMP). The contractor shall in the Government risk management process throughout the PoP by identifying risks to the operational status of the system and recommending appropriate mitigations, and by attending Risk Management Board meetings, which are held monthly.

#### CDRL A009 Risk Management Plan

##### 2.1.5 Meetings and Status Reports

The contractor shall attend and provide status updates in weekly status meetings that provide the Government progress and accomplishments on task, schedule, and any issues.

The contractor shall submit a detailed status report one (1) working day prior to the meeting and detailed minutes to the Government at the conclusion of each meeting. The contractor shall also provide MSRs, which shall include management, technical, and TO execution profiles. The contractor shall provide an updated contractor's Progress and Status Report, and action items with each MSR.

#### CDRL A004 Meeting Minutes

#### CDRL A006 Weekly Status Report

#### CDRL A007 Monthly Status Report

##### 2.1.6 Quality Assurance Program Plan

The contractor shall administer a quality control plan including sub-contractor management in accordance with the Quality Assurance Program Plan.

#### CDRL A008 Quality Assurance Program Plan

##### 2.1.7 Meeting Administration

The contractor shall perform the following tasks in support of meetings necessary to perform and plan the contract tasks:

- a. Write and submit calendar invitations.
- b. Record minutes, action items, decisions, and executive summaries.
- c. Arrange for Government bridge phone lines and operate virtual meeting systems such as Defense Collaborative Services (DCS).
- d. Prepare, archive and track agendas.

##### 2.2 Engineering and Testing

The contractor shall conduct the required engineering and testing activities for sustainment and enhancement of the ITSM tools under direction of Government Lead Systems Engineers (LSEs) in the program office in accordance with the E-ITSM Change Management (ChM) Process.

#### CDRL B00F Test Plans/Test Procedures

##### 2.2.1 Engineering Design and Documentation

The contractor shall develop solution designs and associated documentation for the ITSM Tools and interfacing systems. The contractor shall engineer system enhancements while also updating and validating related design documentation, instructions and procedures, and supporting documentation for enterprise solutions. The contractor shall manage all documentation using strict configuration controls. Documentation shall be technically and procedurally sufficient to allow a third party to validate and/or install and configure the specified systems within the MCEN. Systems Administration and Operational guides shall be documented in accordance with Government standards and incorporate Industry Best Practices.

#### CDRL B001 Functional Design Documents

2.2.1.1 The contractor shall consult the E-ITSM Tools Configuration Control Board (CCB)/Change Review Board (CRB) regarding the engineering documentation required to appropriately document the change for each engineering change to the ITSM tool suite.



2.2.1.2 The contractor shall submit draft and final engineering documentation in PfM MCSES engineering document format to the CRB through the E-ITSM Tools Lead System Engineer (LSE) for approval during system enhancement design and prior to implementation.

2.2.1.3 The contractor shall coordinate with the E-ITSM LSE for posting to the Definitive Media Library (DML).

2.2.1.4 The contractor shall submit documents for USMC review IAW Government LSE specified methods.

Contractor deliverables from each of the engineering efforts shall include professional level technical documentation including decision and point papers and complete and accurate diagrams. The contractor shall support the creation and enhancement through a collaborative effort with the Government of specified PfM MCSES engineering documentation that cover following USMC standard system documents:

- D400 Solution Architecture and CONOPS
- D401 Detailed Technical Design
- D403 Detailed Configuration and Installation Guide
- D405 Solution Components
- D406 Engineering and Operating Guidelines
- D408/SSS Requirements Document
- D409 Functional Test Plan
- D410 Implementation Guide
- D411 Data Architecture
- Requirements Traceability Matrix (RTM)
- TST509 Test Plans (including supporting test cases, test scripts and use cases)
- Diagrams and technical drawings (including logical, physical, wiring, data flow, and topological)
- Site Cut sheets and Site Documentation
- DoD Risk Management Framework (RMF) documentation and artifacts including (but not limited to):
  - Continuous Monitoring Strategy Document
  - Security Assessment Plan (SAP)
    - Hardware & Software lists
    - Ports, Protocols, and Services Document
    - Interfaces & Interconnections Document
    - ATO Boundary Document
    - Data Flow Diagram
    - Security Controls
    - Test Plan
    - Continuity Plan
  - Security Assessment Report (SAR)
    - Finalized Continuous Monitoring Plan
    - Finalized Security Controls
    - Source Code Review
    - Risk Assessment Report (RAR)

CDRL B004 Detailed Technical Design

CDRL B005 Detailed Configuration and Installation Guide

CDRL B006 Solution Components

CDRL B007 Engineering and Operating Guidelines

CDRL B008 Functional Test Plan

CDRL B009 Implementation Guide

CDRL B00A Data Architecture

CDRL A00E Requirements Traceability Matrix

CDRL B00B TST509 Test Plan

CDRL B00C Diagrams and Technical Drawings

CDRL B00D Site Cut sheets and Site Documentation  
CDRL B00E DoD Risk Management Framework documentation

#### 2.2.2 Cybersecurity

The Marine Corps obtains the authorization to release packages for the ITSM toolset through the RMF process per security related guidelines provided in Section 6.2 to support requirements throughout Section 2 of this document.

2.2.2.1 The contractor shall provide security requirements identification, analysis, allocation, and tracking support utilizing DoD Risk Management Framework (RMF) documentation as required.

2.2.2.2. The contractor shall mitigate any security related issues or incidents that may introduce security risks or that do not comply with existing security related policies, regulations, or standards in order to maintain an ATO for all components of the Marine Corps ITSM Tool and component systems.

2.2.2.3 The contractor shall mitigate all issues that may impact the security and authorization of the Marine Corps ITSM Tool. The contractor shall conduct identification analysis, allocation, and tracking support in accordance with DoD RMF.

2.2.2.4 The contractor shall provide security requirement documentation as required and comply with cybersecurity guidelines. The contractor shall enter A&A information and supporting artifacts into the Marine Corps Certification and Accreditation System Tool (MCCAST) system.

#### CDRL B003 Security Requirement Documentation

2.2.2.4.1 The contractor shall develop and update all engineering documentation and artifacts for accreditation packages, scanning, and remediation of findings.

2.2.2.4.2 The contractor shall provide required security SCAN reports and Plan of Action and Milestones (POA&Ms) within establish timeframes. The contractor shall submit updates to existing accreditation packages to accompany all changes to components within EEVE, ZONE A, and EITC enclaves.

2.2.2.4.3 The contractor shall create new accreditation packages for all components outside the ZONE A and EITC enclaves, supported by the Government Cybersecurity (CY) staff where Government approvals and inputs are required by policy as needed.

2.2.2.4.4 The contractor shall ensure the ATO is retained through all Marine Corps ITSM upgrades and capability improvements

2.2.2.4.5 The contractor shall ensure that the ATO is retained through maintenance and operation activities and USMC CY policy changes.

#### CDRL A00B Cybersecurity Requirements Artifacts

#### 2.2.3 Remedy Upgrade

2.2.3.1 The contractor shall perform maintenance and sustainment activities, as required, to ensure the ITSM tool suite remains updated with current software versioning. The contractor shall perform the update in all USMC ITSM tool environments.

2.2.3.2 The contractor shall serve as the Information Systems Security Manager and ensure that the system is configured and documented to support the renewal and retention of an ATO for new system versions and all effected environments.

2.2.3.3 The contractor shall document the system upgrade as an engineering change utilizing the documentation and review requirements listed in Section 2.2.1. The contractor shall develop a test plan (including supporting test cases,

test scripts and use cases) to verify functionality of upgraded features and ensure that previous out-of-the-box and custom functionality is retained.

#### CDRL B002 Test Plan

2.2.3.4 The contractor shall design, develop and maintain a new equipment training (NET) package for all software upgrades and new integrations prior to release. The contractor shall include user's guides in the production deployment of new services.

#### CDRL A00C New Equipment Training Package

2.2.3.5 The contractor shall conduct NET prior to solution deployment.

2.2.3.6 The contractor shall maintain the ITSM toolset availability according to the ITSM Tool Suite Key Performance Parameters (KPPs) as referenced in the ITSM Tool Requirements document. Availability issues caused by USMC actions are not in the scope of this objective. Advanced Technical Problems/Issues data shall be compiled in the weekly and monthly status reports.

#### CDRL A00F Advanced Technical Problems/Issues Report

##### 2.2.4 Module Enhancements and Improvements

The contractor shall perform enhancement and improvement activities, as required, for modules that support the below listed processes. The contractor shall apply the existing ITSM tool enhancement process and work with the Change and Release Process Owner to continually refine and improve that process for broad use across the Marine Corps. The contractor shall ensure that enhancements are properly evaluated, approved, documented, tested, deployed and supported. The contractor shall conduct enhancement engineering for the system to support system changes approved by the Change Advisory Board (CAB). For current detailed ITSM tool requirements on these processes, refer to the ITSM Tool Requirements document in Attachment 1:

- a. Incident Management (IM)
- b. Request Fulfillment (RqF) and Remedy Work Orders (WOs)
- c. Service Catalog Management (SCM)
- d. Change Management (ChM)
- e. Service Asset and Configuration Management (SACM)
- f. Knowledge Management (KM)
- g. Problem Management (PM)
- h. Identity and Access Management (IdAM)
- i. Service Level Management (SLM)
- j. Continual Service Improvement (CSI)

##### 2.2.5 Engineering Changes to Remedy Functions

The contractor shall engineer changes to existing ITSM tool suite through implementation of new and improved BMC component products within the Remedy tool suite family purchased by the Marine Corps. This functionality might include improvements to provide enhancements to self-service incident and knowledge management, social media, and service catalog access functionality utilizing location, role, and preferences to guide users to Remedy resources with formless requests, context-aware services, and crowd sourced collaboration. Specific Remedy components to be supported are:

- Remedy ITSM
- Remedy Single Sign On (RSSO)
- Smart Reporting
- Digital Work Place (DWP)
- Smart IT
- Custom Modules including:
  - Contracts
  - IT Procurement Request and Approval System (ITPRAS)
  - Remedy to Net Interface (RNI)

- Definitive Media Library (DML)
- Technical Refresh (TechRefresh)
- Product Ordering

#### 2.2.6 Asset Discovery Integration

The contractor shall design, develop, document, and implement asset discovery integration and normalization rules, processes, and solutions to support integrating data from asset discovery solutions that provide visibility of network connected assets. The solution shall provide auto-population of Remedy Atrium CIs with discovered data. The contractor shall identify, implement and integrate additional Asset Scanning technologies with current E-ITSM tool suites. The proposed enhancements shall be subject to Government review and approval before work begins to design or implement the enhancement.

#### 2.3 ITSM Tool Suite Operations and Maintenance

The Marine Corps seeks technical support to operate and maintain the current ITSM tool suite that enables the Marine Corps to deliver IT service management functions to its user base. This section describes the administrative activities required for the daily operations and maintenance of the ITSM tool suite.

The ITSM tools and related infrastructure include virtual machines, physical servers, database servers, application instances, and supporting software such as plug-ins and middleware on both unclassified and classified networks. The MCCOG has daily operational responsibilities for the ITSM tool suite which is hosted from the EITC located in Kansas City, MO, but maintained remotely from Quantico, VA.

2.3.1 The contractor shall conduct operations and sustainment activities related to the hosted ITSM applications including software and application level patching. Upon identifying a need for ITSM tool suite maintenance, the identifying party (Government or contractor) will be responsible for documenting the need for issue prevention, issue resolution, or toolset modification via the USMC BMC Remedy ticketing system. The contractor is not responsible for the maintenance of the HCS hosting infrastructure on which many of the ITSM tool components depend. The contractor is also not responsible for the operations and sustainment activities of the operating system or database management system (DBMS) software on which the ITSM applications reside in the HCS hosting environments. The contractor is responsible for coordinating with the HCS database administrators (DBAs) to support the management of the ITSM tool associated databases hosted within the HCS managed DBMS.

2.3.1.1 The contractor shall perform routine Checks: run daily health checks on applications and databases, monitor the email message queue, all CMDB integration jobs, and database backup processes.

2.3.1.2 The contractor shall hold daily Operations Team Meetings to identify performance trends

2.3.1.3 The contractor shall perform monthly checks after monthly server patches run regression testes on system to verify system performance functionality.

2.3.1.4 The contractor shall change passwords every six months for all service and database accounts. This includes reconfiguration of database connection strings in all application servers on all enclaves.

2.3.1.5 The contractor shall provide Outage Support and Troubleshooting for ITSM outages and any required coordination with BMC support resources 24 hours per day/seven days per week.

2.3.1.6 The contractor shall ensure the Operations Team provides the tasks below for enhancements they were not directly involved with creating or resolving of issues:

- a. Unit and Regression testing in the Zone A enclave
- b. Deployment of the fix or enhancement in uProd and cProd
- c. Creation and coordination of CRQ process including presenting of CRQ to MCCOG CAB
- d. Code Review of workflow or form enhancements
- e. Management of all CBT and Job Aid links within Remedy
- f. During Early Life Support, Tier 1 and Tier 2 support and training for the customer.

2.3.1.7 The contractor shall, after major deployments:

- a. Perform regression testing to verify full functionality of the deployed change and to identify any potential, unintended impacts.
  - b. Perform database performance checks to identify any long-running queries and invalid objects
  - c. Address any unusual findings and define and implement resolutions
- 2.3.1.8 The contractor shall deploy patches, hotfixes, upgrades, and enhancements in the following order:
  - a. EEVE Lab
  - b. Training Stack
  - c. Zone A
  - d. uProd
  - e. cProd
- 2.3.1.9 The contractor shall apply the following categorizations to all enhancements, patches, upgrades to ITSM tools as determined by C2 Systems Remedy Government Lead:
  - a. Minor – users will not notice the change, or the changes affect a small group of users
  - b. Medium – user will notice a short interruption in service caused by the change due to a mid-tier cache flush
  - c. Major – requires an ITSM outage to implement change
- 2.3.1.10 The contractor shall perform restoration services, within the following timeframes 98% of the time each month, on these tools once notified through verbal notification or ticket creation by MCCOG. The Recovery Time Objective (RTO) Threshold is eight (8) hours (Monday through Sunday; Government Holidays included) / Objective two (2) hours. The contractor shall provide post incident documentation to capture root cause and lessons learned to identify any procedural or process improvements that will be applied to mitigate future risk of breaches of the RTO SLA. The contractor's recovery process shall include:
  - 2.3.1.1.10.1 The contractor shall create incident tickets to record service interruptions.
  - 2.3.1.1.10.2 The contractor shall reprioritize current work efforts and assignment of appropriate engineers for recovery efforts until service is fully restored.
  - 2.3.1.1.10.3 The contractor shall configure the RTO service targets and the SLA compliance in the BMC Remedy Service Level Management (SLM) Module enabling SLA compliance report generation.
  - 2.3.1.1.10.4 Once service is restored, the contractor shall open a related problem ticket and document the root cause of the outage in the Remedy Problem ticket.
  - 2.3.1.1.10.5 The contractor shall document lessons learned from the service interruption.
- 2.3.1.11 The contractor shall provide ad-hoc reports within five (5) working days of the request. The contractor shall use the USMC ITSM tool suite reporting tool Business Intelligence Reporting Tool (BIRT) and the BMC Self –Monitoring Analysis and Reporting Technology (SMART) Reporting tool to develop these reports. The contractor shall develop workflows to route customer report requests to the appropriate support group queue.
- 2.3.1.12 The contractor shall operate the system to ensure it continues to operate in accordance with the requirements document. For detail ITSM tool requirements, refer to the ITSM Tool Requirements document in Attachment 1.
- 2.3.1.13 The contractor shall perform the following incident prevention monitoring checks to maintain database health and performance:
  - a. Daily Database System Checks
    - i. Monitor alert log for errors
    - ii. Check for session blocking and database locks
    - iii. Verify scheduled daily jobs run successfully
  - b. Weekly Database Checks
    - i. Monitor table space utilization and growth
    - ii. Monitor data file size and available drive space
    - iii. Run diagnostics queries to identify performance issues
    - iv. Check for invalid database object

- c. Monthly Database Checks
  - i. Capture table space/data file growth rates and compare to historical rates

#### 2.3.2 Incident Management (IM)

The contractor shall monitor the ITSM toolset queue and respond to requests in the USMC BMC Remedy ticketing system. The contractor shall document all tickets, with detailed resolution steps, for every ticket that is escalated.

2.3.2.1 The contractor shall work as part of the Incident Resolution team (identified by the Battle Captain in accordance with documented processes and procedures) to ensure restoration of services as quickly as possible for all major incidents associated with the ITSM toolset.

2.3.2.2. The contractor shall keep the MCCOG S-3/C2 Systems section informed of status on all tickets through proper ticket documentation, daily status reports, email, and direct communications.

2.3.2.3 The contractor shall maintain queue management of Remedy, Remedy Developer, and Remedy Reporting.

2.3.2.4 The contractor shall ensure all tickets are acknowledged, assigned and worked in a timely manner.

2.3.2.5 The contractor shall notify the appropriate engineer, developer or administrator a SLA is about to breach and requires attention.

2.3.2.6 The contractor shall run SLA reports weekly to track compliance for SLA purposes.

2.3.2.7 The contractor shall team with MCCOG S-3/C2 Systems in managing the Remedy team queue and coordinating the deployment of fixes.

#### 2.3.3 Request Fulfillment (RqF)

The contractor shall monitor the ITSM toolset support request queue and respond to requests in the USMC BMC Remedy ticketing system. The contractor shall also document all tickets, with detailed resolution steps, for every ticket that is escalated.

#### 2.3.4 Service Catalog Management (SCM)

The contractor shall provide the identification and integration of existing services which could be offered within the USMC On-Line Enterprise IT Service Catalog.

2.3.4.1 The contractor shall develop a workflow that captures the relevant use cases and business needs to meet USMC requirements and routes the requests to the appropriate queues for approval and development

2.3.4.2 The contractor shall monitor the enhancement requests and evaluate templates for manually created work orders to identify services being performed on a regular basis for considered additions to the E\_ITSM Enterprise Service Catalog Portal.

#### 2.3.5 Service Asset and Configuration Management (SACM)

The contractor shall provide Asset Administration Support for individual and mass Configuration Item (CI) generation and population. In support of asset administration, the contractor shall perform CI auditing and reporting activities, as requested by asset management teams and to account for establishment of, and changes to, BMC Remedy foundation data.

#### 2.3.6 Module Maintenance and Sustainment

The contractor shall perform maintenance and sustainment activities, as required, for modules and tickets that support the below listed processes. The contractor shall maintain the system to ensure it continues to operate in accordance with the requirements document. For detailed ITSM tool requirements on these processes, refer to the ITSM Tool Requirements document in Attachment 1:

- a. Incident Management (IM)
- b. Request Fulfillment (RqF) and Remedy Work Orders (WOs)
- c. Service Catalog Management (SCM)

- d. Change Management (ChM)
- e. Service Asset and Configuration Management (SACM)
- f. Knowledge Management (KM)
- g. Problem Management (PM)
- h. Identity and Access Management (IdAM)
- i. Service Level Management (SLM)
- j. Continual Service Improvement (CSI)

2.3.6.1 The contractor shall maintain both OOTB and customized functionality within Remedy ITSM Suite, Atrium CMDB, Smart IT, DWP, Smart Reporting, custom applications and external data source integrations required to support USMC Enterprise ITSM processes.

2.3.6.2 The contractor shall ensure patching of Java and Tomcat to resolve security vulnerabilities.

2.3.6.3 The contractor shall deploy and test new patches as soon as they are released.

2.3.6.4 The contractor shall use the USMC release and change management process to validate, document, plan and coordinate the deployment of patches.

2.3.6.5 The contractor shall track enhancement activities.

2.3.6.6 The contractor shall execute daily database health checks to ensure proper database backups are kept in all enclaves.

2.3.6.7 The contractor shall notify the HCS database team when a scheduled backup fails to resolve the issue.

2.3.6.8 The contractor shall run database performance tasks after every Remedy path and upgrade.

2.3.6.9 The contractor shall review database performance to help identify long running queries and provide appropriate solutions.

2.3.6.10 The contractor shall track foundation data changes via change tickets.

2.3.6.11 The contractor shall provide unit and regression testing services and production deployment of all custom objects and workflow developed by the Development Team for all module maintenance and sustainment changes.

## 2.4 Enhancement of ITSM Training Materials

As operations and maintenance activities occur which alter the interfaces and/or workflows of the ITSM Tools Suite, support is required to update and mature existing ITSM Process New Equipment Training (NET) packages and individual training materials. Materials requiring updates include computer based training (CBT), Procedures/Work Instructions (PWI), Just-In-Time videos (JIT), Job Aids, and Knowledge Articles for the Marine Corps ITSM processes, workflows, and ITSM tool suite. Existing training materials will be provided as GFI. Updates to training materials shall follow the Marine Corps Systems Approach to Training (SAT) Users Guide for classroom and self-paced instruction and MarineNet Courseware configuration and enhancement Technical Requirements for CBTs. Each shall be Shareable Content Object Reference Model (SCORM) Compliant and also have the ability to be hosted in a Learning Management System (LMS).

CDRL A00C New Equipment Training Package  
CDRL A00D Training Materials

2.4.1 The contractor shall deliver the code/editable version of each NET package and training component. The contractor shall provide configuration and enhancement of MarineNet hosting submission documentation and process, including, but not limited to, technical support and documentation updates. The contractor shall furnish all files required to launch and track SCORM 2004-compliant CBT modules from an LMS including:

- a. HyperText Markup Language (HTML) File

- b. Manifest File
- c. JavaScript File
- d. Other exported files (.xsd files)

2.4.2 The contractor shall mature and update the training documentation to coincide with major changes to ITSM tools suite and processes such as tools upgrade, major ITSM process improvements, and tool enhancements.

2.4.3 The contractor shall develop new training documentation such as CBTs, Just in Time Videos, and Job Aids as necessary to coincide with major changes to ITSM tools suite and processes such as tools upgrade, major ITSM process improvements, and tool enhancements.

#### 2.4.3.1 Enhancement of ITSM Tools CBTs

The contractor shall configure a new CBT module or enhance an existing CBT module for new ITSM processes, business processes, or ITSM tools. The CBT shall be similar in complexity to the existing CBTs provided as GFI for the existing processes. The module shall include an assessment to measure a student's understanding of the module's content. The contractor shall submit a draft storyboard for Government approval prior to CBT configuration or enhancement. The contractor shall provide the code/editable version of the CBT. The contractor shall assist the Government in configuration and enhancement of MarineNet hosting submission documentation and process. Training materials shall follow the MarineNet Courseware Configuration Technical Requirements for CBTs. Each shall be Shareable Content Object Reference Model (SCORM) Compliant and have the ability to be hosted in a Learning Management System (LMS).

#### 2.4.3.2 Enhancement of ITSM Tools JITS

The contractor shall configure a new JIT or enhance an existing JIT for new ITSM processes, business processes, or ITSM tools. The JIT shall be similar in complexity to the existing JITs provided as GFI for the existing processes. The contractor shall provide a draft script for Government approval prior to JIT configuration and enhancement. If applicable, the contractor shall provide the code/editable version of the JIT. Upon Government acceptance, the contractor shall load the JIT into Remedy Help for user access.

#### 2.4.3.3 Configuration and Enhancement of ITSM Tools Job Aids

The contractor shall configure a new ITSM Job Aid or enhance an existing ITSM Job Aid for new ITSM processes, business processes, or ITSM tools. The Job Aid shall be similar in complexity to the existing Job Aids provided as GFI for the existing processes. The contractor shall provide the sequenced draft script and screen shots for Government approval prior to Job Aid configuration and enhancement. If applicable, the contractor shall provide the editable version of the Job Aid. Upon Government acceptance, the contractor shall load the Job Aid into Remedy Help for user access.

2.4.4 The contractor shall conduct training for changes to ITSM tools suite and processes such as tools upgrade, major ITSM process improvements, and tool enhancements.

2.4.5 The contractor shall provide virtual training to USMC operators, maintainers, and stakeholders. The contractor shall plan (in conjunction with the COR), host, and conduct virtual training sessions for the ITSM tools suite modules, custom applications, and ITSM processes not to exceed seven (7) individual two (2) hour sessions per quarter.

### 2.5 ITSM Toolset Training Environment

The Marine Corps seeks an advanced ITSM toolset technical problem prevention and problem resolution capability for the ITSM training environment. The Marine Corps also seeks an advanced ITSM toolset modification capability for the ITSM training environment.

The Marine Corps seeks technical support for daily operational responsibilities for the training stack ITSM toolset hosted in HCS Zone A. The tools and related infrastructure include virtual machines, database servers, application instances, and supporting software such as plug-ins and middleware. The contractor shall have expertise in BMC toolsets.



2.5.1 The contractor shall provide ITSM tools technical support in maintaining the ITSM training stack so it is online and available to conduct ITSM training and User Acceptance Testing.

2.5.2 The contractor shall ensure the training environment mirrors the production environment in terms of application configuration. The contractor shall work with SACM and CMDB teams to ensure that the training environment is populated and kept up to date with configuration data from the production environment.

2.5.3 The contractor shall maintain configuration management (CfM), including ITSM Tools component and supporting software, and operational procedures for the training environment.

2.5.4 The contractor shall acknowledge Advanced Technical Problems/Issues and respond to the related tickets within two (2) hours of verbal notification and/or ticket creation by MCCOG. The response shall come from a contractor employee. The contractor's relevant technical SME that has acknowledged the related incident/problem ticket must provide verbal or written notification to the Government operational POC. The contractor shall submit written updates (including summary of problem/issue or requirement, actions taken in the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion) to the Government operational POC until the problem/issue is resolved. These written updates shall be provided, at a minimum, for 95% of all such occurrences. Advanced Technical Problems/Issues data shall be compiled in the weekly and monthly status reports.

#### CDRL A00F Advanced Technical Problems/Issues Report

#### 2.6 ITSM Toolset Configuration and Enhancement Environment

The Marine Corps is establishing an advanced ITSM toolset enhancement capability implemented as an ITSM tools configuration and enhancement Environment within the Enterprise Engineering and Verification Environment (EEVE). The Marine Corps also seeks an ITSM tools configuration and enhancement Environment sustainment capability for the ITSM tools configuration and enhancement Environment upon establishment.

2.6.1 The contractor shall maintain the ITSM tools configuration and enhancement Environment within the EEVE at MCB Quantico, VA utilizing EEVE hardware, software, and infrastructure. The ITSM tools configuration and enhancement Environment includes virtual machines, database servers, application instances, and supporting software such as plug-ins and middleware. This environment currently consists of 15 servers and 7 databases with the following general descriptions:

- 3 Application servers (MS Windows 2012 R2)
- 2 Mid-tier servers (MS Windows 2012 R2)
- 2 Smart Reporting servers (MS Windows 2012 R2)
- 2 Digital Work Place Application server (MS Windows 2012 R2)
- 2 Digital Work Place Catalog server (RHEL 7.8)
- 2 Smart IT server (Windows 2012 R2)
- 1 Definitive Media Library file server (RHEL 7.8)
- 1 Database server (RHEL 7.8)
- 7 Oracle Database Instances (Oracle 12c on RHEL 7.8)

2.6.2 The contractor shall perform all ITSM tools configuration and enhancement Environment Work implementation and changes utilizing the EEVE Change Management process. The contractor shall describe the modifications or enhancements, if any, of the tools configuration and enhancement environment required allowing it to fulfill its mission of providing an effective tools configuration and enhancement environment for the EITC production environment.

2.6.3 The contractor shall maintain the ITSM tools configuration and enhancement Environment available to support system enhancement efforts.

2.6.4 The contractor shall assess the hardware and software configuration of the ITSM tools configuration and enhancement Environment and conduct a capability comparison against the EITC production environment with respect to the configuration and enhancement of the environment's suitability and effectiveness as an environment for producing ITSM tool products for the EITC. The assessment will enable the contractor to perform remediation

tasks as necessary to ensure the ITSM tools configuration and enhancement Environment mirrors the production environment. As the Release and Deployment Management (RDM) and ChM processes mature for ITSM Tool engineering, all solution changes will be developed in the EEVE lab prior to deployment into Zone A, the training environment, and production.

2.6.5 The contractor shall maintain CfM including hardware, software, networking, and operational procedures for the tools configuration and enhancement environment. The contractor shall provide an audit of all Remedy Application Infrastructure Configuration Items in the Configuration and Enhancement Environment at the start of the period of performance.

2.6.6 The contractor shall provide ITSM tools technical support to the Government EEVE lab manager in maintaining the ITSM tools configuration and enhancement environment so it is online and available to conduct ITSM tool enhancement and configuration.

2.6.7 The contractor shall evaluate all changes to be applied to the ITSM toolset production environment within the ITSM tools configuration and enhancement environment prior to submitting change proposals for production implementation.

2.6.8 The contractor shall acknowledge Advanced Technical Problems/Issues and respond to the related tickets within two (2) hours of verbal notification and/or ticket creation by the operator. The response shall come from a contractor employee. The contractor's relevant technical SME that has acknowledged the related incident/problem ticket must provide verbal or written notification to the Government operational POC. The contractor shall submit written updates (including summary of problem/issue or requirement, actions taken in the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion) to the Government operational POC until the problem/issue is resolved. These written updates shall be provided, at a minimum, for 95% of all such occurrences. Advanced Technical Problems/Issues data shall be compiled in the weekly and monthly status reports.

#### CDRL A00F Advanced Technical Problems/Issues Report

#### 2.7 ITSM Tool Suite Enhancement

The Marine Corps seeks support for enhancement of the ITSM tools suite. Some of the existing tools may require upgrades or enhancements during the PoP and additional supporting tools may require implementation to support ITSM process enhancement. New system enhancement projects will focus on the capabilities listed below and may span several of the process areas.

Optional CLINs are defined below. These CLINs describe new capabilities which may be exercised at the Government's discretion to design, enhance, configure, customize, test, implement, and document new ITSM capabilities, or tools to support additional processes, that may be required to perform IT service management on behalf of the Marine Corps. The timing of the option CLINs and placement within subsequent option years represents the Government's best estimates for when those services will be required.

2.7.1 The contractor shall document all changes and place them under USMC CfM utilizing the documentation and review requirements listed in Section 2.2.1. The contractor shall use strict CfM for all hardware, software, documentation, and deliverables.

2.7.1.1 (Option) The contractor shall support migration of the ITSM Tool Suite, or integration of the suite, into a cloud hosting environment (e.g. future cloud provider network), and major system level upgrades for the ITSM Tool Suite itself (e.g. migration to Remedy Helix or another product suite).

2.7.1.2 (Option) The contractor shall create a capability within the ITSM Tool Suite to automate the process of onboarding and offboarding personnel.

2.7.1.3 The contractor shall provide integration support for other tools that support related activities such as risk management, or project management. These integrations will automate the receiving and/or sending of data between the ITSM Tool Suite and the targeted tools. Other tools specifically targeted for integration are as follows:

2.7.1.3.1 (Option) The contractor shall develop an integration with Marine Corps Network Event Management solutions. The intent of this integration is to support better management of assets associated with network events.

2.7.1.3.2 (Option) The contractor shall develop an integration with Jira. The intent of this integration is to support project management associated with ITSM processes.

2.7.1.3.4 (Option) The contractor shall develop an integration with Contract Management Systems. The intent of this integration is to support the better association of procurement data to managed hardware and software assets.

2.7.1.3.5 (Option) The contractor shall develop an integration with the DLA DODAAC system. The intent of this integration is to ensure updated location and address codes are used in managing and tracking physical assets and delivery of services.

2.7.1.3.6 (Option) The contractor shall develop an integration with the Enterprise Staging and Warehousing processing system. The intent of this integration is to ensure hardware asset birth records are properly entered and updated in the CMDB.

2.7.1.3.7 (Option) The contractor shall develop an integration with the Total Force Structure Management System (TFSMS). The intent of this integration is to ensure Marine Corps organizational structures are maintained within the CMDB for association with assets and services.

2.7.1.3.8 (Option) The contractor shall develop an integration with RSA Archer (MCCAST). The intent of this integration is to ensure Marine Corps systems' components are properly associated with managed assets within the CMDB.

2.7.1.4 (Option) The contractor shall automate the processing of software requests to speed the delivery and deployment of software to users. This would include the ability to integrate the request fulfillment process with the software deployment tool for end user software requests. The solution may include a workflow that includes procurement processes and license management and all appropriate approval steps.

2.7.1.5 (Option) The contractor shall consolidate current IT products and services ordering processes into a single point of entry. The current process within the Marine Corps to procure hardware and software involves many steps that are mostly disjointed and not a part of a cohesive process. Implementing an enhancement within the ITSM tool to automate a workflow surrounding the entire process would help to streamline the process and create efficiencies that would save time and resources.

2.7.1.6 (Option) Service Level Monitoring

The contractor shall enhance the existing ITSM Tool Suite to enable the authorized user to monitor customer usage and service usage for each service utilizing the existing Marine Corps Event Management System (MEMS) solution.

### 3.0 General Requirements

3.1 The contractor shall communicate all official electronic correspondence using official Government email accounts.

3.2 The contractor shall document all changes under the scope of this task and place them under USMC configuration management (CfM).

3.3 The contractor shall use strict CfM for all hardware, software, documentation, and deliverables.

3.4 The contractor shall acknowledge Advanced Technical Problems/Issues and respond to the related tickets within two (2) hours of verbal notification and/or ticket creation by MCCOG. The contractor shall respond within two hours during the regular Government business hours. However, during major incidents, live operational support may include outside business hours to support urgent break fixes. The response shall come from a contractor employee. The contractor's relevant technical SME that has acknowledged the related incident/problem ticket must provide verbal or written notification to the Government operational POC. The contractor shall submit written

updates (including summary of problem/issue or requirement, actions taken in the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion) to the Government operational POC until the problem/issue is resolved. These written updates shall be provided, at a minimum, for 95% of all such occurrences.

3.5 The contractor shall engineer updates to the system to ensure it continues to operate in accordance with the requirements document. For detail ITSM tool requirements, refer to the ITSM Tool Requirements document in Attachment 1.

### 3.6 Adherence to Marine Corps Documentation Standards

The contractor shall conform to Government provided Marine Corps ITSM process and tool documentation standards. This documentation, includes process guides, design documentation, site documentation, Technical Data Packages (TDPs), Functionality Definition Documents (FDDs), Procedures/Work Instructions (P/WIs), training documentation and artifacts, and defines the process environment and detailed tool design that form the Marine Corps ITSM configuration baseline.

3.6.1 The contractor shall provide content and recommend updates, based on lessons learned and analysis of Government-approved changes.

3.6.2 The contractor shall update these documents based only on Government-approved changes. The contractor shall ensure that documentation accurately and comprehensively reflects the system state in every environment where it exists.

3.6.3 The contractor shall adhere to ChM, SACM, and RDM requirements.

3.6.4 The contractor shall provide all technical deliverables in Microsoft Office Suite editable format (including document content such as figures and tables) to facilitate continual improvement by the Government. The contractor may compress technical information into formats such as, but not limited to, bmp, html, pdf, jpeg, or png within primary deliverables, but if so, shall provide the original, modifiable file for each compressed image or data element. For example, the Government must be able to change the source and destination of workflow arrows, alter the text in process activity boxes, and change the connections of circuit diagrams.

3.6.5 The contractor shall document all designs, configurations, settings, and other data relevant to the technical work performed in the TDPs. The contractor shall provide additional supporting products in any case where the TDPs and other existing artifacts are not appropriate media for any particular technical details.

All Requests for Change (RFCs) must be approved before any system changes can be injected into each environment (EEVE, Training, Zone A, and EITC) as releases are developed across the RDM process. RFCs typically require a two-week lead time for Change Advisory Board (CAB) approval. After initial CAB approval of a proposal change, the release is developed and tested within RDM, which could take an additional two weeks or more. This means that RFCs will have to be drafted and submitted approximately four weeks before a proposed change to the network to meet future contractor delivery schedules.

### 3.7 Coordination with Concurrent Efforts

Conduct of ITSM process training, implementation, installation, configuration, and training of other tools may be accomplished in parallel with other vendors. The Government desires a unified, integrated ITSM solution.

3.7.1 The contractor shall support the Government in achieving this goal by coordinating efforts and schedules with other efforts and vendors through the Government POC. Where conflicts arise, the contractor shall present them to the Government for adjudication.

3.7.2 The contractor shall support integration by including all design and configuration details in deliverables which become Government property. The contractor shall allow other Government support contractors to attend all meetings, workshops, conference calls, and training events, and to review draft documentation related to this TO facilitating an open exchange of information.

3.7.3 The contractor shall support Government-facilitated transition efforts to introduce awardees of other contracted ITSM support tasks into planning and operations. These efforts will be those that ensure the ITSM Tool Suite continues to support other ITSM related processes and tools and will require interaction with other contract support and government personnel.

### 3.8 Process Adherence

Although Marine Corps E-ITSM processes and tools are meant to guide and support the delivery of services by a variety of different programs and organizations, the Marine Corps ITSM Tools team must follow the same guidance in its work on the Marine Corps ITSM Tool Suite itself.

3.8.1 The contractor shall conform to Marine Corps ITSM processes while carrying out the tasks herein. The contractor shall work in accordance with the following process restrictions as well as all additional guidance listed in Marine Corps E-ITSM process documentation:

3.8.1.1 The contractor shall associate IT service-related data with the services in the Marine Corps Service Catalog. Document all incidents and incident response activities related to contractor tasks in the USMC Remedy Incident module.

3.8.1.2 The contractor shall make no changes to operational systems, or other systems under ChM control, without a Government-approved RFC which describes that specific change.

3.8.1.3 The contractor shall ensure that the configurations of the processes, tools, and services as related to contractor tasks are documented in the Marine Corps ITSM Configuration Management System (CMS). The CMS includes the USMC Remedy Atrium CMDB, multiple USMC SharePoint sites, and the USMC Definitive Media Library (DML).

3.8.1.4 The contractor shall bundle changes to the ITSM tools suite into thoroughly documented release packages IAW USMC documentation standards.

3.8.1.5 The contractor shall complete and support all RFC packages for the USMC ITSM tool suite that must go through the Marine Corps ITSM processes.

### 3.9 SME Skill Set Requirements

3.9.1 The contractor shall staff ITSM tools O&S support with senior level engineers with knowledge and experience in interfacing and enabling technologies including:

- Incident Management
  - BMC Remedy Incident Management
  - BMC Remedy Service Request Module
- Change Management
  - BMC Remedy Change Management
- Configuration Management
  - BMC Remedy Atrium CMDB
  - BMC Remedy Asset Management
- Release and Deployment Management
  - BMC Remedy Release Management
- Service Catalog Management
  - BMC Remedy Service Request Module
- Service Request Fulfillment Management
  - BMC Remedy Service Request Module
  - Work Order Management Module
- Knowledge Management

- BMC Remedy Knowledge Management
- Problem Management
  - BMC Remedy Problem Management
- Identity and Access Management
  - BMC Remedy Access Management
- Service Level Management
  - BMC Remedy Service Level Management
- Non-process specific
  - BMC Remedy SMART Reporting/Analytics
  - BMC Remedy Development
  - BMC Remedy Administration
  - Oracle Database Administrator (DBA)
  - Training Development Software (e.g. Captivate, Camtasia)

### 3.9.2 SME System Access Requirements

The contractor personnel who will be working on production systems and supporting live and development environments shall meet the following criteria:

- a. The contractor personnel requiring standard system access shall have a fully adjudicated SECRET clearance at the start of their performance.
- b. The contractor personnel requiring administrative access to systems shall have a fully adjudicated SECRET clearance at the start of their performance.
- c. The contractor personnel requiring administrative access to systems shall be IAT level II certified at the start of their performance.
- d. The contractor personnel performing systems engineering activities shall be IAT level III certified at the start of, and for the duration of, their performance.

### 3.9.3 Personnel Access Requirements

The contractor shall complete appropriate forms and processes in order to obtain valid access to systems and facilities. The forms and processes include, but are not limited to: System Authorization Access Request (SAAR), access to Operational Directive (OpDir), Marine Corps Certification & Accreditation Support Tool (MCCAST), access badges for MCSC, request for SIPRNet access, contractor Verification System (CVS), and Joint Personnel Adjudication System (JPAS). The contractor shall ensure adherence to the requirements listed in DoDI 8500.2 and DOD 8570.01M; specifically, contractor personnel who will be working on the production systems and supporting live environments are required to have and maintain IAT Level II certification. All personnel shall conduct initial and annual IA refresher awareness training in accordance with MARADMIN 257/12.

### 3.9.4 Code Review

The contractor shall document all system modifications according to the USMC documentation standards. The contractor shall provide content to be approved by the Government.

### 3.9.5 Contract Risk Management Process

The contractor shall implement a risk management process that aligns its assessment methodology the E-ITSM Service RMP to achieve with program and contract objectives. The contractor shall submit reports summarizing candidate risks, identifying their likelihood, and potential consequences of each candidate risk. The contractor shall develop and share these risks with the Government for consideration by the Risk Management Board (RMB).

3.9.5.1 The contractor shall provide the summary reports via appropriate SME attendance/participation in meetings as required, to include providing input and comments into all phases of risk management collaborations.

3.9.5.2 The contractor will submit candidate risks to the E-ITSM RMB.

3.9.5.3 The contractor will participate in the RMB review and validation process to accurately assess candidate risks, propose mitigations, and effectively manage risks.

### 3.9.6 Certification Requirements

The contractor shall ensure personnel are certified in the following areas in order to demonstrate competency and subject matter expertise as well as comply with federal regulations and directives.

- a. The contractor personnel supporting project management shall have Program Management certifications (PMI PMP or Equivalent).
- b. The contractor personnel supporting cybersecurity related tasks shall have appropriate certifications in accordance with the DoD Directive 8140.01 and Defense Federal Acquisition Regulation Supplement (Reference (c)) subpart 239.71.
- c. The contractor personnel supporting operations and sustainment of the BMC Remedy product suite shall have certifications appropriate for their role such as BMC Certified Associate, BMC Certified Professional, or BMC Certified Expert.
- d. The contractor personnel supporting operations and sustainment of the Oracle database shall have at a minimum Oracle Database Administration Certified Professional or equivalent.
- e. The contractor shall have at a minimum one person with BMC Helix certification.

### 4.0 Government Furnished Equipment (GFE) and Government Furnished Information (GFI)

The Government will provide desk space and telephones within Government facilities for all contractors supporting the objectives, as well as required badges and accesses that have been approved.

#### 4.1 Information

The documents listed below in Table 1, will be made available via the DoD Safe Access File Exchange tool, which can be found at <https://safe.apps.mil/>. To receive the documents, contractors should respond to the POC listed in the RFP and provide a contractor POC name, email address, and phone number. Access information will be sent to the contractor POC. If any additional documents become necessary, please send a request to the contract specialist listed in the solicitation and the documents will be shared if deemed necessary.

**Table 1. GFI Documents**

Item	Qty
Marine Corps Systems Command Order 4130.1	1
Marine Corps Systems Command Technical Review Handbook v1.04	1
Marine Corps ITSM Process Guides	Multiple
ITSM Tool Requirements Document	1
Marine Corps ITSM TDPs	Multiple
Marine Corps ITSM P/WIs	Multiple
Marine Corps ITSM FDDs	Multiple
Marine Corps ITSM Training Documentation	Multiple
Marine Corps Development Documentation (DEVDOC) Standards and Templates	Multiple
PfM MCSSES Engineering Document Templates	Multiple

#### 4.2 Software for Lab

To support the establishment and sustainment of ITSM tools associated with this task, the Government will provide the following software items for use in ITSM tools configuration, enhancement, and test activities:

- BMC Remedy Product Suite
- Microsoft Windows Server
- Kelverion Windows Orchestrator
- Red Hat Enterprise Linux
- Oracle Database
- Seamless Data Pump
- PKI Single Sign On

4.2.1 The contractor shall provide any additional configuration, testing, and enhancement tools identified as required within their Technical Approach.

#### 4.3 Hardware

To support the establishment and sustainment of ITSM tools associated with this task, the Government will provide the following hardware items for contractor resources that need recurring access to the MCEN Secret environment:

- MCEN-S End User Device (EUD)

## 5.0 Contractor Furnished Items and Responsibilities

### 5.1 General

5.1.1 The contractor shall furnish all supplies, computer equipment, facilities, and services that are not listed under Section 4 required to perform work under this PWS. The contractor shall furnish a fully functional and licensed workstation (laptop preferred) for each individual supporting this PWS to be imaged as a MCEN unclassified End User Device (EUD). Additionally, those individuals providing onsite development support in the EEVE lab shall require a fully functional and licensed workstation to be imaged as an EEVE Lab EUD.

5.1.2 The contractor shall supply all required peripherals (monitor, keyboard, mouse, cables software licensing, etc.). Each EUD laptop shall comply with the hardware and software license specifications maintained by End User Hardware Services portfolio, PFM MCSES.

5.1.3 The contractor provided EUDs shall include the hardware and software licenses needed to run the MCEDS image for each contractor assigned to support this effort. The contractor shall provide the authentication credentials for BIOS/UEFI configurations. Once imaged and joined to the MCEN or EEVE Lab domains, the device will remain under Government Configuration Control. At the end of the contract, or if the device needs to be replaced, the contractor shall provide the devices to the Government to wipe it and validate all Government data has been cleaned from the storage drives.

### 5.2 Security Requirements

This contract will require the contractor to have a Secret Facility Clearance and will require certain contractors to obtain and maintain classified access eligibility. The contractor shall have a valid Secret Facility Clearance prior to classified performance. The prime contractor and all sub-contractors (through the prime contractor) shall adhere to all aspects of 32 CFR Part 117 NISPOM. All personnel identified to perform on this contract shall maintain compliance with Department of Defense, Department of the Navy, and Marine Corps Information and Personnel Security Policy to include completed background investigations (as required) prior to classified performance. This contract shall include a DoD Contract Security Classification Specification (DD-254) as an attachment. Certain contractors will be required to perform IT-I/II duties that will require favorably adjudicated Tier 5/3 Level investigations. The Defense Counterintelligence Security Agency (DCSA) will not authorize contractors to submit the necessary Tier Level investigations solely in support of IT level designation requirements, but are required to submit investigations for those employees requiring both Secret access and IT-II designation. The Government Contracting Activity Security Office (GCASO) is required to submit any required investigations in support of IT-I level designations. The contractor is required to provide a roster of prospective contractor employees performing IT-I duties to the MCSC Contracting Officer's Representative (COR). This roster shall include: full names, Social Security Numbers, e-mail address and phone number for each contractor requiring investigations in support of IT Level designations. The COR will verify the IT-I requirements and forward the roster to the GCASO. Contractors found to be lacking required investigations will be contacted by the GCASO.

Facility Security Officers (FSOs) are responsible for notifying the MCSC AC/S G-2 Personnel Security Office (PERSEC Office) via encrypted e-mail to MCSC\_Security@usmc.mil or 703-432-3374/3952 if any contractor performing on this contract receives an unfavorable adjudication. The FSO must also notify the PERSEC Office, within 24 hours, of any adverse/derogatory information associated with the 13 Adjudicative Guidelines concerning any contractor performing on this contract, if they have been granted an IT designation, issued a CAC, a Government Building Access Badge and/or granted classified access. The FSO shall notify the Government (written notice) within 24 hours of any contractor personnel added or removed from the contract that have been granted IT designations, issued a Common Access Card (CAC) and/or a MCSC Building Badge.

All contractor personnel accessing Marine Corps Systems Command facilities/buildings, must maintain compliance with access control policy identified within MCSCO 5530.2A - Access Control Order. Access into MCSC facilities requires use of a Command facility access badge issued by the PHYSEC Team. Contractor personnel assigned to sit



within MCSC spaces with a dedicated (by name) workspace will be considered “on-site” contractors and may be issued a Green badge with the holder’s photograph. Contractor personnel that frequently visit (three or more times a week) MCSC spaces will be considered “off-site” contractors and may be issued an Orange badge with the holder’s photograph. Issuance of a MCSC facility access badge shall be initiated by the COR using the Badge Request process hosted on the MCSC VIPER website. Vendors may be issued a MCSC facility badge prior to issuance of a CAC or DBID card; however, receipt of an unfavorable response will result in deactivation of any currently issued MCSC facility access badge. All other vendors supporting this contract who do not meet the “Green” or “Orange” badge standards shall be required to have their visit to MCSC notified in advance using the MCSC Visitor Notification System hosted on the MCSC VIPER website. Visitor Notifications shall only be submitted by a MCSC sponsor with access to the MCSC VIPER website. Visitors who arrive at MCSC facilities without an approved Visitor Notification on file shall be turned away unless a MCSC escort with a “White”, “Powder Blue”, or “Green” badge can be reasonably coordinated. Vendors possessing an “Orange” badge are not authorized to escort visitors without an approved Visitor Notification on file. All “Green” and “Orange” badges will be programmed with unescorted access into approved MCSC facilities Monday through Friday from 0630-1700. Unescorted access outside of these times to include federal holidays, furloughs, shutdowns, etc. is restricted. For additional questions regarding MCSC facility access requirements, you may contact the PHYSEC Team at [mcsc\\_physicalsecurity@usmc.mil](mailto:mcsc_physicalsecurity@usmc.mil) or by calling 703-432-3964/3909.

### 5.3 Common Access Card (CAC) Requirement

The COR will identify and only approve those contractor employees performing on this contract that require CACs in order to perform their job function. In accordance with Headquarters, United States Marine Corps issued guidance relative to Homeland Security Presidential Directive – 12 (HSPD-12), all personnel must meet eligibility criteria to be issued a CAC. In order to meet the eligibility criteria, contractor employees requiring a CAC must obtain and maintain a favorably adjudicated Personnel Security Investigation (PSI). Prior to authorizing a CAC, the employee’s Defense Information System for Security (DISS) record must indicate a completed and favorably adjudicated PSI or (at a minimum) that a PSI has been submitted and accepted (opened). The minimum acceptable investigation is a T-1 or a National Agency Check with Written Inquiries (NACI). If a contractor employee’s open investigation closes and is not favorably adjudicated, the CAC must be immediately retrieved and revoked. CACs are not issued for convenience.

Facility Security Officers (FSOs) are responsible for notifying the MCSC AC/S G-2 Personnel Security Office (PERSEC Office) at 703-432-3490/3952 if any contractor performing on this contract receives an unfavorable adjudication after being issued a CAC. The FSO must also immediately notify the PERSEC Office of any adverse/derogatory information associated with the 13 Adjudicative Guidelines concerning any contractor issued a CAC, regardless of whether a JPAS Incident Report is submitted.

Each CAC is issued with a “ctr@usmc.mil” e-mail account that the individual contractor is responsible to keep active by logging in on a regular basis (at least twice a month), sending an e-mail and clearing any unneeded e-mails. Contractors issued a CAC are prohibited from “auto-forwarding” e-mail from their .mil e-mail account to their .com e-mail account. If the “ctr@usmc.mil” e-mail account is not kept active, G-6 will deactivate the account and the CAC will also lose its functionality. Contractor employees shall solely use their Government furnished “ctr@usmc.mil” e-mail accounts for work supporting the USMC, conducted in fulfillment of this contract, and shall not use a contractor supplied or personal e-mail account to conduct official U.S. Government business. The use of a contractor or personal e-mail account for contractor business or personal use is allowed, but only when using cellular or a commercial internet service provider.

If a contractor loses their eligibility for a CAC due to an adverse adjudicative decision, they have also lost their eligibility to perform on MCSC contracts.

### 5.4 Marine Corps Enterprise Network (MCEN) Computer Access

Contractor personnel accessing Marine Corps Systems Command Computer systems, must maintain compliance with United States Marine Corps Enterprise Cybersecurity Manual 007 Resource Access Guide. Contractor personnel will submit a DD 2875, and completion certificates for the CYBERC course located on MarineNet located at <https://www.marinenet.usmc.mil>. The CYBERC course consist of the DOD Cyber Awareness Challenge and Department of the Navy Annual Privacy Training (PII). Contractors will have to create a MarineNet account in order to acquire the required training.

MCEN IT resources, if provided, are designated for official use only and other limited authorized purposes. DoD military, civilian personnel, consultants, and contractor personnel performing duties on MCEN information systems may be assigned to one of three position sensitivity designations.

- 1) ADP-I (IT-1): Favorably adjudicated T-5, T5R, (formerly known as Single Scope Background Investigation (SSBI)/SSBI Periodic Reinvestigation (SBPR)/SSBI Phased Periodic Reinvestigation (PPR))
- 2) ADP-II (IT-2): Favorably adjudicated T-3, T3R, (formerly known as Access National Agency Check and Inquiries (ANACI)/ National Agency Check with Law and Credit (NACLC)/Secret Periodic Review (S-PR))
- 3) ADP-III (IT-3): Completed T-1, (formerly known as National Agency Check with Inquiries (NACI))

All privileged users (IT-1) must undergo a T-1 investigation regardless of the security clearance level required for the position. Privileged users must maintain the baseline Cyberspace Workforce Information Assurance Technical (IAT) or Information Assurance Manager (IAM) relating to the position being filled. Privileged users are defined as anyone who has privileges over a standard user account as in system administrators, developers, network administrators, code signing specialist and Service Desk technicians.

All MCEN users must read, understand, and comply with policy and guidance to protect classified national security information, Controlled Unclassified Information (CUI), and prevent unauthorized disclosures in accordance with United States Marine Corps Enterprise Cybersecurity Manual 007 Resource Access Guide and CJCSI 6510.01F.

#### 5.5 MCEN Official E-mail usage

MCEN IT resources are provided for official Government use only and other limited authorized purposes. Authorized purposes may include personal use within limitations as defined by the supervisor or the local Command. Auto forwarding of e-mail from MCEN-N to commercial or private domains (e.g., Hotmail, Yahoo, Gmail, etc.) is strictly prohibited. E-mail messages requiring either message integrity or non-repudiation are digitally signed using DoD PKI. All e-mail containing CUI, an attachment, or embedded active content must be digitally signed.

MCEN users will follow specific guidelines to safeguard CUI, including PII or Health Insurance Portability and Accountability Act (HIPAA) information. Non-official e-mail is not authorized for and will not be used to transmit CUI to include PII or HIPAA information. Non-official e-mail is not authorized for official use unless under specific situations where it is the only mean for communication available to meet operational requirements. This can occur when the official MCEN provided e-mail is not available but must be approved prior to use by the Marine Corps Authorizing Official (AO).

All personnel will use DoD authorized PKI certificates to encrypt e-mail messages if they contain any of the following:

1. Information categorized as Controlled Unclassified Information (CUI).
2. Any contract sensitive information that normally would not be disclosed to anyone other than the intended recipient. This is also considered CUI.
3. Any privacy data, PII, or information intended for inclusion in an employee's personal file or any information that would fall under the tenets of MSGID: DOC/5 USC 552A. Personal or commercial e-mail accounts are not authorized to transmit unencrypted CUI, PII or HIPAA.
4. Any medical or health data, to include medical status or diagnosis concerning another individual.
5. Any operational data regarding status, readiness, location, or deployment of forces or equipment.

#### 6.0 Applicable Publications (Current Editions)

The contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures. The Marine Corps ITSM documents listed in Table 1 provide essential programmatic information that needs to be considered in the contractor's initial proposal.

## 6.1 Compliance Documents

The contractor is required to perform in compliance with the most recent version of the following requirements, standards, and guidelines.

### 6.1.1 The following documents or references are applicable to this PWS to the extent specified herein:

- National Industrial Security Program Operating Manual (NISPOM – DoD Directive 5220.22-M)
- DFARS 252.232-7003
- DFARS 252.211-7003
- FAR 9.5
- MIL-HDBK-61A
- DoD Directive 5000.01, The Defense Acquisition System
- DoD 8750 series of instructions

### 6.1.2 Security Related Guidance

- Federal Information Security Management Act (FISMA) of 2002
- DoDD 8500.01E, Information Assurance (IA), 24 Oct 2002 (current as of 23 Apr 2007)
- DoD 8570.01M, Information Assurance Workforce Improvement Program, Incorporating Change 3, January 24, 2012
- CJCSI 6510.01F, Information Assurance and Computer Network Defense, 09 February 2011
- SECNAVINST 5000.2E, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, 01 September 2011
- DoD 5200.2-R, Personnel Security Program
- DoDD 8000.01, Management of the DoD Information Enterprise
- NFPA 75 (Standard for the Protection of Information Technology Equipment)
- MCO 5239.1, Marine Corps Information Assurance Program (MCIAP)
- MCO 5239.2A Marine Corps Cyber Security Program (MCCSP), 18 July 2012
- MARADMIN 257/12 UPDATES TO ANNUAL CYBER AWARENESS TRAINING
- MARADMIN 639/08, MCBUL 5239 USMC IA VULNERABILITY MANAGEMENT (IAVM) PROGRAM
- IETF RFC 4346 - The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006.
- The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs), Ver 1.5 11 August 2011 ([http://www.commoncriteriaportal.org/pp\\_OD.html](http://www.commoncriteriaportal.org/pp_OD.html))
- WARP Ports and Protocol Description
- SIAT RMF Process Guidance document (draft)

### 6.1.3 Standards

- MIL-PRF-49506 (Performance Specification - Logistics Management Information); November 1996
- MIL-HDBK-470A (Designing and Developing Maintainable Products and Systems, Vol 1); 04 December 1997
- MIL-HDBK-781A (Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production); April 1996
- ASME Y14.34-2008 (Associated Lists)
- ASME Y14.100-2004 (Reaffirmed 2009) (Engineering Drawing Practices)
- ASTM F1166-07 (Standard Practice for Human Engineering Design for Marine Systems, Equipment, and Facilities)
- EIA-625 (Requirements for Handling Electrostatic Discharge-Sensitive (ESDS) Device)
- EIA-649-A, April 2004 (National Consensus Standard for Configuration Management)
- Capabilities Maturity Model Integration (CMMI) v1.3, November 2010.
- Information Technology Infrastructure Library (ITIL) v3 or later

### 6.1.4 Other Guidance

- DoD 5000.02, Operation of the Defense Acquisition System, 02 December 2008
- Defense Acquisition Guidebook (<https://dag.dau.mil/Pages/Default.aspx>)

- DoD 8500 series of instructions
- DoDI 8510.01
- MCSC Order 4130.1, Configuration Management Policy
- MCSC Order 5000.3 Naval SYSCOM Risk Management Policy
- IEEE/EIA 12207.0-1996, IEE Standard for Information Technology- Software Life Cycle Processes
- ISO/IEC 15289:2011, Systems and software engineering – Content of life cycle process information products (documentation)
- DoD Guide to Uniquely Identifying Items, Ver.2.5, 15 Sept 2012 (replaces all previous versions)
- DISA Policy and Guidance [https://cyber.mil/policies-guidance/ASN\(RD&A\)Guidebook for Acquisition of Naval Software Intensive Systems](https://cyber.mil/policies-guidance/ASN(RD&A)Guidebook%20for%20Acquisition%20of%20Naval%20Software%20Intensive%20Systems), Ver 1.0, September 2008; (<http://acquisition.navy.mil/rda/content/view/full/6079>)
- MCSC Acquisition Guidebook (MAG), V1.0, March 2012
- Marine Corps Systems Command Technical Review Handbook V1.04, April 2009
- DoD Joint Travel Regulations
- Department of Defense Architecture Framework Version 2.0
- Department of Defense Enterprise Service Management Framework (DESMF)

## 7.0 Acronyms/Glossary

ACL	Access Control List
A&A	Assessment and Authorization
ATO	Authority to Operate
B/P/S	Base/Post/Station
BYOD	Bring Your Own Device
C&A	Certification and Accreditation
CAB	Change Advisory Board
CAE	Client Automation Enterprise
CBT	Computer Based Training
CDR	Critical Design Review
CDRL	Contract Data Requirements List
cEITC	Classified Enterprise Information Technology Center
CfM	Configuration Management
ChM	Change Management
CI	Configuration Item
CITDB	Configuration Item Technical Data Base
CLIN	Contract Line Item Number
CMDB	Configuration Management Database
CMP	Configuration Management Plan
CMS	Configuration Management System
COE	Concept of Employment
COR	Contracting Officer Representative
CPR	Critical Process Review
cPROD	Production environment on the secure network
CRB	Change Review Board
CRM	Comment Resolution Matrix
CS3	Customer Service and Strategic Sourcing
CSI	Continual Service Improvement
CVS	Contractor Verification System
CY	Cybersecurity
DBA	Database Administrator
DC I	Deputy Commandant for Information
DD254	Department of Defense Contract Security Requirement List
DDS-M	Data Distribution System – Modular

DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DoDI	Department of Defense Instruction
DON	Department of the Navy
EITC	Enterprise Information Technology Center
E-ITSM	Enterprise Information Technology Service Management
EM	Event Management
ESD	Enterprise Service Desk
FAR	Federal Acquisition Regulation
FDD	Functional Design Document
FISMA	Federal Information Security Management Act
FTE	Full-Time Equivalents
FY	Fiscal Year
GAT	Government Acceptance Test
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GIG	Global Information Grid
GOGO	Government-Owned, Government-Operated
GPO	Government Printing Offices
HCS	Hybrid Cloud Services
HPNA	HP Network Automation
HQMC C4	Headquarters Marine Corps Command, Control, Communications, and Computers
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IM	Incident Management
IMS	Integrated Master Schedule
IPT	Integrated Product Team
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITPRAS	Information Technology Procurement Request Review/Approval System
ITSM	Information Technology Service Management
JIT	Just in Time Videos
JPAS	Joint Personnel Adjudication System
KM	Knowledge Management
KO	Contracting Officer
KPP	Key Performance Parameter
LMS	Learning Management System
LSE	Lead Systems Engineer
MAC	Mission Assurance Category
MCSC	Marine Corps Systems Command
MARFOR	Marine Forces
MCB	Marine Corps Base
MCCAP	Marine Corps Certification and Accreditation Process
MCCAST	Marine Corps Certification & Accreditation Support Tool
MCCOG	Marine Corps Cyber Operations Group
MCEIAD	Marine Corps Enterprise Information Assurance Directive
MCIEE	Marine Corps Information Environment Enterprise
MFCC	Marine Forces Cyberspace Command
MCEN	Marine Corps Enterprise Network
MCEN-N	Marine Corps Enterprise Network - Non-classified Internet Protocol (IP) Router Network
MCEN-S	Marine Corps Enterprise Network – Secret Internet Protocol (IP) Router Network
MCI	Marine Corps Installation
MCIENT	Marine Corps Information Enterprise
MCSC	Marine Corps Systems Command
MITSC	Marine Air-Ground Task Force (MAGTF) Information Technology Support Center

MS	Microsoft
MSR	Monthly Status Report
NET	New Equipment Training
NetOps	Network Operations
NIPRNet	Non-classified Internet Protocol Router Network
NGEN	Next Generation Enterprise Network
NLT	No Later Than
NNMi	Network Node Manager interface
ODC	Other Direct Costs
OLA	Operating Level Agreement
OpDir	Operational Directive
O&S	Operations and Sustainment
OSI	Open Systems Interconnection
PEO Digital	Program Executive Office Digital and Enterprise Services
PbM	Problem Management
PDR	Preliminary Design Review
PfM MCSES	Portfolio Management Marine Corps Supporting Establishment Systems
POA&M	Plan of Action & Milestone
PoP	Period of Performance
PPR	Preliminary Process Review
P/WI	Procedures/Work Instructions
PMP	Program Management Plan
PWS	Performance Work Statement
QA	Quality Assurance
QAPP	Quality Assurance Program Plan
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
RDM	Release and Deployment Management
RFC	Request for Change
RMB	Risk Management Board
RMP	Risk Management Plan
RNOSC	Regional Network Operations and Security Center
RqF	Request Fulfillment
RTO	Recovery Time Objective
SLA	Service Level Agreement
SA	Situational Awareness
SAAR	System Account Access Request
SACM	Service Asset and Configuration Management
SAT	Systems Approach to Training
SCCM	System Center Configuration Manager
SCM	Service Catalog Management
SCORM	Shareable Content Object Reference Model
SE	Systems Engineering
SECNAVINST	Secretary of the Navy Instruction
SETR	Systems Engineering Technical Review
SLM	Service Level Management
SLT	Service Level Target
SPM	Service Portfolio Management
SRM	Service Request Management
SVR	System Verification Review
TAR	Tool Access Request
TDLC	Technical Delivery Life Cycle
TDP	Technical Data Package
TO	Task Order
UC	Underpinning Contracts

uEITC	Unclassified Enterprise Information Technology Center
uPROD	Production environment on the non-secure network
USMC	United States Marine Corps
WBS	Work Breakdown Structure

**Appendix A - Performance Requirements Summary**

PWS Paragraph	Task	Performance Standard	Acceptable Quality Levels (AQL)	Surveillance Method / By Whom
2.1 Program Management	The contractor shall submit initial IMS, WBS, RMP, PMP, and staffing plan as Deliverables within the established timeframe.	The contractor shall submit initial IMS, WBS, RMP, PMP, and staffing plan IAW the deliverables timeframe as stated in DD-1423(CDRL) 100% of the time.	0% failure to submit initial IMS, WBS, RMP, PMP, and staffing plan as Deliverables within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated DD-1423(CDRL)
2.1: Program Management	The contractor shall submit updated IMS within the established timeframe.	The contractor shall submit updated IMS IAW the deliverable timeframe as stated in DD-1423(CDRL) 100% of the time.	0% failure to submit updated IMS IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in DD-1423(CDRL)
2.1: Program Management	The contractor shall submit updated WBS and Staffing Plan within the established timeframe.	The contractor shall submit updated WBS and Staffing Plan IAW the deliverable timeframe as stated in DD-1423(CDRL) 100% of the time.	0% failure to submit updated WBS and Staffing Plan IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in DD-1423(CDRL)
2.1: Program Management	The contractor shall submit updated RMP within the established timeframe.	The contractor shall submit updated RMP IAW the deliverable timeframe as stated in DD-1423(CDRL) 100% of the time.	0% failure to submit updated RMP IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in DD-1423(CDRL)
2.1: Program Management	The contractor shall submit weekly status reports within the established timeframe.	The contractor shall submit weekly status reports IAW the deliverable timeframe as stated DD-1423(CDRL) 99% of the time.	1% failure to submit weekly status reports IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in DD-1423(CDRL)
2.1: Program Management	The contractor shall deliver fully functional and effective ad-hoc meeting support and reporting within the established timeframe.	The contractor shall deliver fully functional and effective ad-hoc meeting support and reporting IAW the deliverable timeframe as stated in DD-1423(CDRL) 99% of the time	1% failure to deliver fully functional and effective ad-hoc meeting support and reporting IAW the deliverable within the established timeframe.	Periodic Inspection by the COR on a quarterly basis.
2.1: Program Management	The contractor shall provide Engineering Design/Documentation (DEVDOCS) within	The contractor shall provide Engineering Design/Documentation within the established	0% failure to provide Engineering Design/Documentation	100% Inspection – COR will review Engineering



	the established timeframe.	timeframe 100% of the time.	within the established timeframe.	Design/Documentation on a quarterly basis.
2.1: Program Management	The contractor shall support successful completion of <del>SETR</del> ChM Technical Review events within the established timeframe	The contractor shall support successful completion of ChM Technical Review events within the established timeframe 100% of the time.	0% failure to support successful completion of ChM Technical Review events within the established timeframe.	100% Inspection – COR will review Presentation Materials and Meeting Minutes, Functional Design Documents, Test Plan on a quarterly basis.
2.1: Program Management	The contractor shall submit DoD Risk Management Framework Documentation in support of IA within the established timeframe.	The contractor shall submit DoD Risk Management Framework Documentation in support of IA within the established timeframe 100% of the time.	0% failure to submit DoD Risk Management Framework Documentation in support of IA within the established timeframe.	100% Inspection – COR will continuously monitor IA documentation on a quarterly basis.
2.1: Program Management	The contractor shall submit documents for USMC review IAW approved change and release plans within the established timeframe.	The contractor shall submit documents for USMC review IAW approved change and release plans within the established timeframe 100% of the time.	0% failure to submit documents for USMC review IAW approved change and release plans within the established timeframe.	100% Inspection – COR will review Presentation Materials and Meeting Minutes, Functional Design Documents, Test Plan on a quarterly basis.
2.1: Program Management	The contractor shall administer a quality control plan including sub-contractor management IAW the deliverable QAPP within the established timeframe.	The contractor shall administer a quality control plan including sub-contractor management IAW the deliverable QAPP within the established timeframe 95% of the time.	0% failure to administer a quality control plan including sub-contractor management IAW the deliverable QAPP within the established timeframe.	Periodic Inspection by the COR on a quarterly basis.
2.2: Engineering and Testing	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframe.	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframe 95% of the time. All RMF packages shall be at least 90% correct, requiring no greater than 10% rework.	5% failure to submit DoD RMF packages, which are at a minimum 90% correct, requiring no greater than 10% rework, when required due to system changes or security requirements within the established timeframe.	Periodic Inspection – The COR will inspect CY artifacts on a quarterly basis.
2.2: Engineering and Testing	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established	5% failure to submit DoD RMF packages when required due to system changes or security requirements within the established timeframes.	Periodic Inspection – The COR will inspect CY artifacts on a quarterly basis.

	the established timeframes.	timeframes 95% of the time.		
2.2: Engineering and Testing	The contractor shall apply all required security patches or updates as required and remediate any ITSM system functionality affected by such updates within the established timeframes.	The contractor shall apply all required security patches or updates as required and remediate any ITSM system functionality affected by such updates within the established timeframes 95% of the time. Security patches applied within one week of Information Assurance Vulnerability Alert (IAVA) release notice or based on USMC direction.	5% failure to apply all required security patches or updates as required and remediate any ITSM system functionality affected by such updates within the established timeframes.	Periodic Inspection – The COR will inspect CY artifacts on a quarterly basis.
2.2: Engineering and Testing	The contractor shall Ensure that the ATO remains in effect at all times during the PoP within the established timeframes.	The contractor shall Ensure that the ATO remains in effect at all times during the PoP within the established timeframe. 100 % system compliance with RMF, the FISMA, and the Marine Corps Enterprise Information Assurance Directive (MCEIAD).	0% failure to Ensure that the ATO remains in effect at all times during the PoP.	100% Inspection – COR will review IA Artifacts and compliance with the PWS.
2.2: Engineering and Testing	The contractor shall provide the required SCAN reports and Plan of Action & Milestones (POA&Ms) to demonstrate the changes have been implemented correctly within the established timeframes.	The contractor shall provide required SCAN reports and POA&Ms within the established timeframes 100% of the time.	0% failure to provide required SCAN reports and POA&Ms within the established timeframes.	100% Inspection – COR will review IA Artifacts and compliance with the PWS.
2.2: Engineering and Testing	The contractor shall provide ITSM tools functionally capable according to the FDDs for implemented processes within the established timeframes.	The contractor shall provide ITSM tools functionally capable according to the FDDs for implemented processes within the established timeframes 100% of the time.	0% failure to provide ITSM tools functionally capable according to the FDDs for implemented processes within the established timeframes.	100% Inspection – COR will review IMS, WBS and compliance with the PWS.
2.2: Engineering and Testing	The contractor shall engineer system enhancements while	The contractor shall update 100% of associated document	0% failure to engineer and document ITSM tools enhancement	100% Inspection by the COR and Government LSE – Review IMS,

	also updating and validating related documentation in accordance with project schedules.	with each system enhancement effort by scheduled completion date.	capabilities in accordance with the Government approved schedule.	design documentation, and lab system configurations.
2.2: Engineering and Testing	The contractor documentation shall be technically and procedurally sufficient to allow a third party to validate and/or install and configure the specified systems within the MCEN.	The contractor documentation shall be technically and procedurally sufficient 100% of the time by scheduled completion date.	0% failure to delivery technically and procedurally sufficient documentation by the scheduled completion date.	100% Inspection by the COR and Government LSE – Review IMS, design documentation, install and config documents and system configurations.
2.2: Engineering and Testing	The contractor shall consult the E-ITSM Tools Configuration Control Board (CCB)/Change Review Board (CRB) regarding the engineering documentation required to appropriately document the change.	The contractor shall consult the E-ITSM Tools Configuration Control Board (CCB)/Change Review Board (CRB) regarding the engineering documentation required to appropriately document the change 100% of the time	0% failure to deliver documentation to the CCB/CRB for engineering documentation.	100% Inspection by the COR and Government LSE – Review IMS, design documentation, and lab system configurations.
2.2: Engineering and Testing	The contractor shall provide high quality releases based on the Release Impact Rate as defined, where impact is the percentage of incidents per a given release.	The contractor shall provide high quality releases based on the Release Impact Rate Calculation of not more than 15%.	Not more than 15% of production releases in an annual period cause an incident.	Periodic Inspection – COR and LSE will review weekly status report, monthly status report, design documentation, and system configurations
2.2: Engineering and Testing	The contractor shall calculate the release rollback rate percentage as defined where a release must be rolled back to a prior state.	The contractor shall provide high quality releases based on the Release Rollback Rate Calculation of not more than 10%.	Not more than 10% of production releases in an annual period must be rolled back to a prior state.	Periodic Inspection – COR and LSE will review weekly status report, monthly status report, design documentation, and system configurations
2.2: Engineering and Testing	The contractor shall develop and support implementation of deployment plans for engineered changes.	The contractor shall develop and support implementation of deployment plans for engineered changes within the established timeframes 100% of the time.	0% failure to develop and support implementation plans within the established timeframes.	100% Inspection – COR and LSE will inspect the Migration Plan
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall perform restorative maintenance within the established timeframes.	The contractor shall perform restorative maintenance within the established	2% failure to perform restorative maintenance within the established timeframes each month.	Periodic Inspection - COR will review monthly work order logs.

		timeframes 98% of the time each month.		
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall acknowledge tickets after verbal notification and ticket creation by MCCOG related to problems and issues within the established timeframe.	The contractor shall acknowledge tickets after verbal notification and ticket creation by MCCOG related to problems and issues within the established timeframe 95% of the time.	5% failure to acknowledge tickets after verbal notification and ticket creation by MCCOG related to problems and issues within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall provide written updates to the Government operational POC when advanced technical problems/issues are resolved within the established timeframe.	The contractor shall provide written updates to the Government operational POC when advanced technical problems/issues are resolved within the established timeframe 95% of the time.	5% failure to provide written updates to the Government operational POC when advanced technical problems/issues are resolved within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes 98% of the time.	2% failure to restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall maintain ITSM toolset availability (based on contractor caused unplanned downtime) within the established timeframe.	The contractor shall maintain ITSM toolset availability (based on contractor caused unplanned downtime) within the established timeframe 98% of the time.	2% failure to maintain ITSM toolset availability (based on contractor caused unplanned downtime) within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall restore ITSM tools classified under RMF within the established timeframe.	The contractor shall restore ITSM tools classified under RMF within the established timeframe 98% of the time.	2% failure to restore ITSM tools classified under RMF within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall deliver fully functional and effective ad-hoc reporting within the established timeframe.	The contractor shall deliver fully functional and effective ad-hoc reporting within the established timeframe 95% of the time. Ad-hoc report turnaround shall be within 5 working days.	5% failure to deliver fully functional and effective ad-hoc reporting within the established timeframe.	Periodic Inspection – The COR will inspect Ad-Hoc Reports on a quarterly basis.
2.3: ITSM Tool Suite	The contractor shall submit DoD RMF packages when	The contractor shall submit DoD RMF packages when	5% failure to submit DoD RMF packages, which are at a minimum	Periodic Inspection – The COR will inspect

Operations & Maintenance	required due to system changes or security requirements within the established timeframe.	required due to system changes or security requirements within the established timeframe 95% of the time. All RMF packages shall be at least 90% correct, requiring no greater than 10% rework.	90% correct, requiring no greater than 10% rework, when required due to system changes or security requirements within the established timeframe.	IA artifacts on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframes.	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframes 95% of the time.	5% failure to submit DoD RMF packages when required due to system changes or security requirements within the established timeframes.	Periodic Inspection – The COR will inspect IA artifacts on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall apply all required security patches or updates as required and remediate any ITSM system functionality affected by such updates within the established timeframes.	The contractor shall apply all required security patches or updates as required and remediate any ITSM system functionality affected by such updates within the established timeframes 95% of the time. Security patches applied within one week of Information Assurance Vulnerability Alert (IAVA) release notice or based on USMC direction.	5% failure to apply all required security patches or updates as required and remediate any ITSM system functionality affected by such updates within the established timeframes.	Periodic Inspection – The COR will inspect IA artifacts on a quarterly basis.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall Ensure that the ATO remains in effect at all times during the PoP within the established timeframes.	The contractor shall Ensure that the ATO remains in effect at all times during the PoP within the established timeframe. 100 % system compliance with RMF, the FISMA, and the Marine Corps Enterprise Information Assurance Directive (MCEIAD).	0% failure to Ensure that the ATO remains in effect at all times during the PoP.	100% Inspection – COR will review IA Artifacts and compliance with the PWS.
2.3: ITSM Tool Suite Operations & Maintenance	The contractor shall provide the required SCAN reports and Plan of Action & Milestones	The contractor shall provide required SCAN reports and POA&Ms within the	0% failure to provide required SCAN reports and POA&Ms within the established timeframes.	100% Inspection – COR will review IA Artifacts and compliance with the PWS.

	(POA&Ms) to demonstrate the changes have been implemented correctly within the established timeframes.	established timeframes 100% of the time.		
2.4: Enhancement of ITSM Training Materials	The contractor shall provide accurate and complete training material within the established AQL.	The contractor shall provide accurate and complete training material and ensure the training material is in compliance with the planned syllabus and lesson plans within the established AQL 100% of the time.	0% failure to provide accurate and complete training material in compliance with the syllabus and lesson plans within the established AQL.	100% Inspection – COR will review training materials.
2.4: Enhancement of ITSM Training Materials	The contractor shall provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL.	The contractor shall provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL 100% of the time.	0% failure to provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL.	100% Inspection – COR will review training materials.
2.5: ITSM Toolset Training Environment	The contractor shall resolve advanced technical problems/issues in response to tickets received from MCCOG or a verbal or written notification within the established timeframe.	The contractor shall resolve advanced technical problems/issues in response to tickets received from MCCOG or a verbal or written notification within the established timeframe 95% of the time.	5% failure to resolve advanced technical problems/issues in response to tickets received from MCCOG or a verbal or written notification within the established timeframe.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.5: ITSM Toolset Training Environment	The contractor shall provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours and estimated date/time of completion within the established timeframes.	The contractor shall provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion within the established timeframes 95% of the time.	5% failure to provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.5 : ITSM Toolset Training Environment	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems)	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established	2% failure to restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.

	within the established timeframes.	timeframes 98% of the time.		
2.6 : ITSM Toolset Configuration & Enhancement Environment	The contractor shall acknowledge and respond to problem tickets within the established timeframes.	The contractor shall acknowledge and respond to problem tickets within the established timeframes 95% of the time.	5% failure to acknowledge and respond to problem tickets within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.6 : ITSM Toolset Configuration & Enhancement Environment	The contractor shall provide written updates and summary to the Government POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours and estimated date/time of completion until the problem is resolved within the established timeframes.	The contractor shall provide written updates and summary to the Government POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours and estimated date/time of completion until the problem is resolved within the established timeframes 95% of the time.	5% failure to provide written updates and summary to the Government POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion until the problem is resolved within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.6 : ITSM Toolset Configuration & Enhancement Environment	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes 98% of the time.	2% failure to restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.7 : ITSM Tool Suite Enhancement	The contractor shall provide high quality releases based on the Release Impact Rate as defined, where impact is the percentage of incidents per a given release.	The contractor shall provide high quality releases based on the Release Impact Rate Calculation of not more than 15%.	Not more than 15% of production releases in an annual period cause an incident.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.7 : ITSM Tool Suite Enhancement	The contractor shall calculate the release rollback rate percentage as defined where a release must be rolled back to a prior state.	The contractor shall provide high quality releases based on the Release Rollback Rate Calculation of not more than 10%.	Not more than 10% of production releases in an annual period must be rolled back to a prior state.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.7 : ITSM Tool Suite Enhancement	The contractor shall develop and support implementation of deployment plans for engineered changes.	The contractor shall develop and support implementation of deployment plans for engineered changes within the established timeframes 100% of the time.	0% failure to develop and support implementation plans within the established timeframes.	100% Inspection – COR and LSE will inspect the Migration Plan